el/sbk/2007R001178

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon. 10-114 (KSH)
	:	
v.	:	Criminal No. 10-
	:	
KENNETH LOWSON,	:	18 U.S.C. § 371
a/k/a "Money,"	:	18 U.S.C. § 1030(a)(2)(C)
KRISTOFER KIRSCH,	:	18 U.S.C. § 1030(a)(4)
a/k/a "Robert Woods,"	:	18 U.S.C. § 1030(a)(5)(A)
JOEL STEVENSON, and	:	18 U.S.C. § 1343
FAISAL NAHDI	:	18 U.S.C. § 2

INDICTMENT

The Grand Jury in and for the District of New Jersey, sitting in Newark, charges:

COUNT 1
18 U.S.C. § 371
Conspiracy

BACKGROUND

1. At various times relevant to this Indictment:

Wiseguys

a. Wiseguy Tickets, Inc. ("Wiseguys"), a Nevada corporation, used fraudulent misrepresentations and computer hacking to purchase tickets surreptitiously over the Internet to concerts, sporting events, and other forms of live entertainment ("Events") throughout the United States. To achieve this goal, Wiseguys deployed a nationwide computer network that opened thousands of simultaneous Internet connections from across the United States; impersonated thousands of individual ticket

buyers; and defeated online ticket vendors' security mechanisms. When online ticket vendors tried to stop Wiseguys from engaging in this conduct, Wiseguys adapted its methods and continued. Through these fraudulent and unauthorized steps, among others, Wiseguys and its owners made more than $20 million in profits while purchasing more than 1 million tickets to Events nationwide.

b. Wiseguys typically sold the tickets that it bought fraudulently over the Internet to ticket brokers in New Jersey and elsewhere, who in turn sold the tickets to the general public. Wiseguys profited from the fraudulent scheme by charging its customers, the ticket brokers, a percentage mark-up over the face value of the tickets it obtained.

c. At various times between in or about late 2002 and in or about January 2009, Wiseguys employed approximately 10 to 15 people and operated under the names Wiseguys, Seats of San Francisco, Inc. ("SOSF"), Smaug, Inc. ("Smaug"), and Platinum Technologies, Inc. ("Platinum Technologies"), among others. (Wiseguys, SOSF, Smaug, and Platinum Technologies are referred to collectively as "Wiseguys"). At various times during this period, Wiseguys was headquartered in Los Angeles and San Francisco, California.

Defendants

d. Defendant KENNETH LOWSON, a co-founder and part owner of Wiseguys, controlled and oversaw all of the company's operations. Defendant LOWSON directed the computer programmers who created and modified the computer networks and software that Wiseguys used to purchase tickets illegally over the Internet. Defendant LOWSON also reaped the largest share of Wiseguys' profits.

e. Defendant KRISTOFER KIRSCH, a part owner of Wiseguys, was responsible, along with defendant LOWSON, for overseeing the technology that Wiseguys used to obtain Event tickets illegally. Wiseguys' employees reported (either directly or indirectly) to defendant KIRSCH on all matters involving the company's ticket-purchasing software and networks. Like defendant LOWSON, defendant KIRSCH shared in Wiseguys' profits.

f. Defendant JOEL STEVENSON, one of Wiseguys' first employees, was the company's chief U.S.-based computer programmer and systems administrator. Defendant STEVENSON, who reported to defendants LOWSON and KIRSCH, programmed substantial parts of Wiseguys' ticket-purchasing software, including computer code that was intended to defeat security measures that online ticket vendors put in place to prevent automated ticket purchasing. Defendant STEVENSON also oversaw the activities of other Wiseguys programmers in the United States and eastern Europe. In 2008,

Wiseguys paid defendant STEVENSON a salary of approximately $150,000 per year.

g. Defendant Faisal NAHDI was Wiseguys' Chief Financial Officer. Defendant NAHDI, who reported to defendants LOWSON and KIRSCH, oversaw certain aspects of Wiseguys' clandestine ticket-purchasing operations, managed its financial relationships with its broker clients, and interacted with vendors who supported Wiseguys' computer infrastructure. In or about June 2008, defendant NAHDI became the straw owner of the Wiseguys' entity SOSF as part of an effort to conceal both Wiseguys' operations and defendant LOWSON's ownership of Wiseguys. In 2008, Wiseguys paid defendant NAHDI a salary of at least approximately $165,000 per year.

Employees and Contractors

h. B.C., D.E., M.P., J.Z., and B.W. were Wiseguys employees responsible for managing Wiseguys' computer networks, taking ticket orders from brokers throughout the United States, and using Wiseguys' software and computer networks to purchase tickets anonymously over the Internet. In 2008, Wiseguys paid B.C., D.E., M.P., J.Z., and B.W. between approximately $55,000 and approximately $142,000 each.

i. P.S. resided in Bulgaria and was the chief architect and programmer of the software and computer networks that Wiseguys used to purchase tickets. P.S. routinely communicated

with defendant LOWSON regarding how Wiseguys could purchase tickets against the wishes of online ticket vendors without being detected. Wiseguys paid P.S. approximately $1,000 to $1,500 per month during the time that he worked for Wiseguys.

j. F.F. and O.M. were contract employees who also resided in Bulgaria and performed system administration and programming duties for Wiseguys. Wiseguys paid F.F. and O.M. approximately $1,000 to $1,500 per month each during the time that they worked for Wiseguys.

2. At various times relevant to this Indictment:

Online Ticket Vendors

a. Ticketmaster, Telecharge, Tickets.com, Musictoday, Major League Baseball, and LiveNation, among others (individually and collectively "the Online Ticket Vendors"), sold Event tickets over the Internet on behalf of venues (e.g., stadiums and concert halls), promoters, artists, and sports teams. The market in which Online Ticket Vendors sold Event tickets to the general public was known as the primary ticket market ("the Primary Market").

b. Agreements among Online Ticket Vendors, venues, promoters, teams, and artists ("Event Agreements") established the number of tickets available to Online Ticket Vendors for sale to the general public, the prices of those tickets, and the fees that Online Ticket Vendors charged for selling each Event ticket.

Some Event Agreements also required that Online Ticket Vendors conduct "pre-sales," in which certain credit card customers (e.g., American Express Gold Card) or fan club members would receive passwords that gave early opportunities to purchase Event tickets.

c. Online Ticket Vendors typically negotiated and obtained the right to be the exclusive distributors of tickets to the Primary Market for certain Events and the right to define the terms of sale for those tickets. Exclusivity and the right to define the terms of sale were valuable property interests to the Online Ticket Vendors because: (1) visits to their websites generated revenue through ticket sales; (2) there was substantial goodwill value in being the exclusive distributor for Event tickets; and (3) Online Ticket Vendors' reputations in the marketplace depended in part on the public's perception that they could fairly distribute tickets on a first-come, first-served basis.

d. Online Ticket Vendors typically did not receive all of the tickets to an Event to sell to the general public. Venues, promoters, and artists often required that as many as 20 to 50 percent of Event tickets be reserved for artists, corporate sponsors, or the venues themselves.

e. The prices that Event Agreements established for Event tickets on the Primary Market often were lower than the potential

resale price of the Event tickets on the open market. Artists and venues often required Online Ticket Vendors to charge such prices on the Primary Market for many reasons, including to allow more fans to afford and seek to buy Event tickets and to increase the likelihood that Events would sell out. This pricing strategy also contributed to the growth of a "Secondary Market," where ticket brokers and others would resell tickets purchased from Online Ticket Vendors on the Primary Market for the highest price the market would bear.

f. To ensure fair access to Event tickets on the Primary Market, Online Ticket Vendors generally limited the number of seats that an online purchaser could obtain per event. Online Ticket Vendors also prohibited the purchase of Event tickets on their websites for commercial re-sale (i.e., the purchase by ticket brokers). Online Ticket Vendors required their Internet customers to accept these rules before buying Event tickets.

Online Ticket Sales

g. Online Ticket Vendors managed nationwide computer networks to distribute Event tickets. Ticketmaster's network, for example, consisted of three data centers, nine web servers, and thousands of retail access points nationwide, including approximately two dozen access points in New Jersey. Access points were integral parts of Ticketmaster's network.

h. To purchase tickets, customers searched the Online Ticket Vendors' networks by Event and venue and could request to purchase a certain number of tickets at a particular cost up to the maximum number of permitted tickets for that Event. If available tickets matched a customer's request, Online Ticket Vendors offered the customer a single set of seats – identified by row, section, and seat number – for sale. The customer would then have a limited number of minutes either to purchase the tickets or discard the tickets and perform a new search for different tickets. During this period, the tickets under consideration were unavailable to any other user. Online Ticket Vendors did not reserve more than one set of tickets per customer at a time.

i. Because the Event Agreements required Online Ticket Vendors to sell tickets on a first-come, first-served basis, Online Ticket Vendors invested millions of dollars in technologies that created virtual "queues" to serve would-be Internet purchasers in the order that they arrived. On these systems, how quickly an on-line purchaser reached the virtual queue would determine which tickets that user could purchase, or whether the user could purchase tickets at all. For the most popular Events, tenths of a second could mean the difference between purchasing seats in the first 10 rows of an Event or not being able to see the Event at all.

j. High demand for the most popular Events, low Primary Market ticket prices, and the widespread use of the Internet to purchase tickets caused many of the most popular events to sell out within minutes. Premium tickets to these events, i.e., the seats nearest to the stage, could sell out within 30 seconds.

k. In an effort to fulfill their obligation to distribute tickets fairly, Online Ticket Vendors restricted access to the portions of their websites that could actually be used to purchase Event tickets. Online Ticket Vendors specifically prohibited computer programs that purchased tickets automatically, such as "bots," "worms," "spiders," and "crawlers," from accessing their sites. To enforce these restrictions and to protect their webpages from automated ticket purchasing software, Online Ticket Vendors used computer code and software that was designed to detect and prohibit automated programs from accessing Online Ticket Vendors' computer servers.

CAPTCHA

l. CAPTCHA, which stood for "Completely Automated Public Turing test to tell Computers and Humans Apart," was one of the technologies that Online Ticket Vendors used to prevent the automated programs from accessing their websites. CAPTCHA served as a gatekeeper by requiring would-be Internet ticket purchasers to type answers to questions that only humans could answer. Specifically, would-be ticket purchasers attempting to purchase

Event tickets online would encounter "CAPTCHA Challenges." These challenges were pictures of a word (or of various letters, numbers, or characters), such as those seen below in Figure 1,

Fig. 1

that required users to type the same characters into a text box before they were permitted past the gatekeeper to purchase Event tickets. The characters of CAPTCHA Challenges were distorted so that they would be recognizable to the human eye but confusing to computers, even to computers using an automated reading technology known as Optical Character Recognition ("OCR").

m. CAPTCHA Challenges are delivered to a user's computer as a computer file. Each CAPTCHA Challenge computer file has a unique identifier that distinguishes it from all other CAPTCHA Challenges ("the File ID"). A computer can identify the File ID without opening and reading the CAPTCHA Challenge.

n. To make clear the purpose of CAPTCHA, Online Ticket Vendors using CAPTCHA technology on their websites routinely added Terms of Service that expressly stated that users were not permitted to access a CAPTCHA-protected website using automated software. For example, Ticketmaster used language, as seen below

in Figure 2, stating that access was unauthorized to users of automated programs:

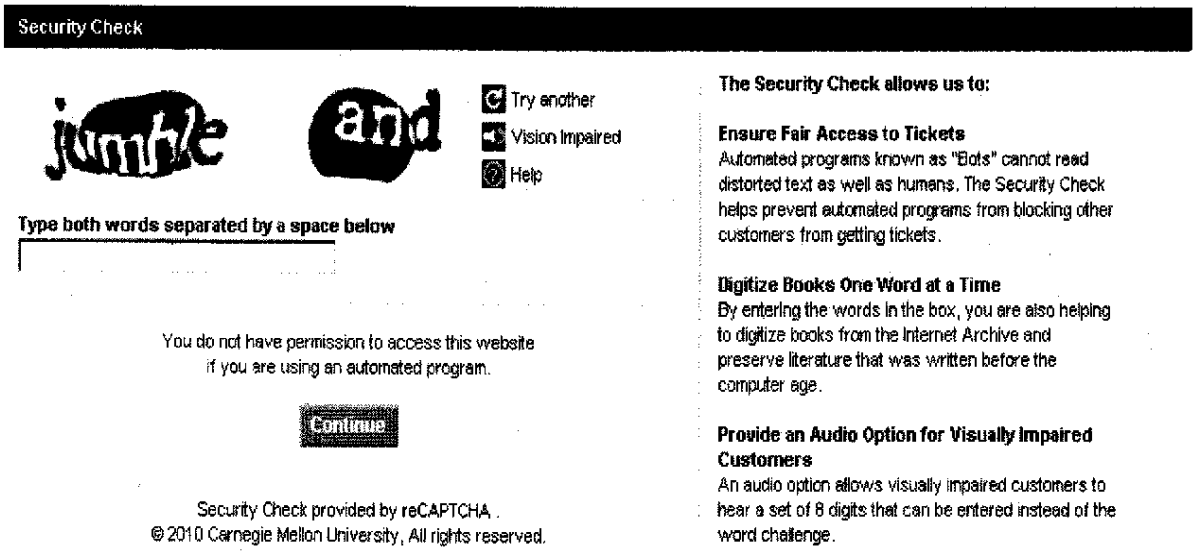


Fig. 2.

Audio CAPTCHA

o. Audio CAPTCHA was a technology that Online Ticket Vendors and other companies used alongside CAPTCHA to accommodate visually impaired customers. Instead of presenting distorted characters for a human user to see and then type in response, audio CAPTCHA Challenges required human users to listen to and type spoken numbers, which were often distorted with significant background noise, before users could purchase Event tickets. Again, the distortion was intended to make the numbers decipherable to a human ear but not to a computer, even one using voice recognition technology.

reCAPTCHA

p. ReCAPTCHA was a company that administered a free CAPTCHA service that third parties could subscribe to and use in their own businesses. ReCAPTCHA's subscribers included Ticketmaster and the social networking website Facebook, among others. Ticketmaster switched to using reCAPTCHA's services after its own CAPTHCA system became less successful in blocking automated ticket purchasing. When Ticketmaster needed to administer a CAPTCHA Challenge to a would-be ticket buyer, Ticketmaster would transmit a unique code to reCAPTCHA, which then sent a CAPTCHA Challenge to the ticket buyer on Ticketmaster's behalf.

Additional Steps to Combat Automation

q. Ticketmaster implemented an additional technology, known as "Proof-of-Work," to combat automated ticket purchases. Proof of Work was a computer program that attempted to slow down computers that were attempting to purchase large volumes of tickets simultaneously.

r. Ticketmaster also sent cease and desist letters to companies that they suspected were using automated programs to defeat CAPTCHA technologies and to purchase tickets. For example, as early as on or about August 10, 2005, Ticketmaster's legal counsel contacted defendant LOWSON and Wiseguys regarding the improper purchase of tickets. Additionally, on or about June

2, 2008, and June 5, 2008, Ticketmaster contacted companies hosting Wiseguys' computers to demand that Wiseguys stop using automated programs to access Ticketmaster's servers.

s. Ticketmaster and other Online Ticket Vendors also blocked Internet Protocol ("IP") addresses of computers that appeared to be using automated programs to access and attack their websites. (An IP address is a unique series of numbers (e.g., 94.23.82.23) assigned to a computer that is connected to the Internet. Generally, each computer connected to the Internet has its own, unique IP address.) For example, on or about December 16, 2007, Ticketmaster blocked thousands of IP addresses that Wiseguys was using to defeat CAPTCHA Challenges and to automate the purchase of Event tickets from Ticketmaster.

t. Online Ticket Vendors also reviewed ticket purchase transactions for popular Events and cancelled transactions that appeared to have been accomplished with automated software.

u. In total, Online Ticket Vendors spent more than $1 million to prevent, detect, and combat the use of automated software on their servers.

THE CONSPIRACY

3. From in or about late 2002 through on or about January 30, 2009, in California, in the District of New Jersey, and elsewhere, defendants

KENNETH LOWSON,
a/k/a "Money,"
KRISTOFER KIRSCH,
a/k/a "Robert Woods,"
JOEL STEVENSON, and
FAISAL NAHDI

did knowingly and intentionally conspire and agree with each other, P.S., and others to commit an offense against the United States, that is:

(1) to devise a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and to transmit and cause to be transmitted by means of wire communications writings, signs, signals, and sounds in interstate and foreign commerce in furtherance of such scheme and artifice, contrary to Title 18, United States Code, Section 1343;

(2) to intentionally access computers without authorization and exceed authorized access, and thereby obtain information from protected computers, namely computers used in and affecting interstate and foreign commerce and communication, for purposes of commercial advantage and private financial gain, contrary to Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(i);

(3) to knowingly and with intent to defraud access protected computers, namely, computers in and affecting interstate and foreign commerce and communication, without authorization and exceed authorized access, and by means of such conduct to further the intended fraud and obtain things of value, contrary to Title 18, United States Code, Sections 1030(a)(4) and 1030(c)(3)(A); and

(4) to knowingly cause the transmission of programs, information, codes, and commands, and as a result of such conduct, to intentionally cause damage without authorization to protected computers, namely computers in and affecting interstate and foreign commerce and communication, and as a result of such conduct, thereby cause loss to one or more persons during any one-year period aggregating at least $5,000 in value, contrary to Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B)(i).

OBJECT OF THE CONSPIRACY

4. It was the object of the conspiracy to profit by defrauding Online Ticket Vendors and others through circumventing computer code and surreptitiously obtaining and then reselling Event tickets that Online Ticket Vendors would not otherwise sell to Wiseguys.

MANNER AND MEANS OF THE CONSPIRACY

5. It was part of the conspiracy that defendants LOWSON and KIRSCH would identify Online Ticket Vendors whose websites could be exploited to purchase Event tickets by defeating security measures on the websites.

6. It was further part of the conspiracy that defendants LOWSON and KIRSCH would advertise on online forums for computer programmers who could write automated software to defeat CAPTCHA.

7. It was further part of the conspiracy that defendants LOWSON and KIRSCH would hire P.S., O.M., and others ("the Contract Hackers") to write automated software that would defeat security measures used by the Online Ticket Vendors, including CAPTCHA.

8. It was further part of the conspiracy that defendant LOWSON would interview former employees of Online Ticket Vendors to learn how Online Ticket Vendors protected their websites from automated programs.

9. It was further part of the conspiracy that defendants LOWSON, KIRSCH, and STEVENSON would direct the Contract Hackers and other Wiseguys employees to explore ways of arriving first in the virtual ticket lines used by Online Ticket Vendors to sell Event tickets, including by:

a. employing OCR and other mechanisms to defeat CAPTCHA Challenges;

b. acquiring the source code, or underlying computer code, that Online Ticket Vendors used to protect their websites from automated programs;

c. testing the vulnerability of security encryption that Online Ticket Vendors used to prevent immediate and direct access to the "buy page", the final step in the ticket-buying process (i.e., access without responding to CAPTCHA Challenges at all, whether automatically or otherwise);

d. implementing "hacks" to get around computer code that Online Ticket Vendors used to protect their websites from automated programs; and

e. using "backdoors" and "tricks" to enable automated software to purchase tickets.

The Automated Ticket Purchasing System - the CAPTCHA Bots

10. It was further part of the conspiracy that defendants LOWSON, KIRSCH, and STEVENSON would work with the Contract Hackers to develop an automated ticket purchasing system (the "CAPTCHA Bots"). The CAPTCHA Bots was a nationwide network of computers that Wiseguys used to purchase, or "pull," thousands of tickets per minute by:

a. monitoring the Online Ticket Vendors' websites for the exact moment that tickets to popular Events went on sale ("Watchers");

b. opening thousands of connections to Online Ticket Vendors at the instant that tickets to popular Events went on sale;

c. defeating CAPTCHA Challenges in a fraction of a second, as opposed to the approximately 5 to 10 seconds (for visual challenges) or 30 seconds (for audio challenges) that it might take an average human user to respond to similar CAPTCHA Challenges;

d. defeating Proof-of-Work challenges from Ticketmaster by responding to them in a way that did not slow down the CAPTCHA Bots;

e. presenting Wiseguys employees with a list of hundreds of the best tickets for each Event to choose from – as opposed to the limited number of tickets that a true human user could review at one time; and

f. filling in all of the fields necessary to complete a ticket purchase, including customer credit card information and false e-mail addresses.

11. It was further part of the conspiracy that to enable the CAPTCHA Bots to purchase tickets automatically, Wiseguys:

a. Downloaded hundreds of thousands of possible CAPTCHA Challenges from reCAPTCHA. To obtain these CAPTCHA Challenges anonymously, Wiseguys wrote a computer script that disguised the

origin of the download requests by impersonating would-be users of Facebook, which also subscribed to reCAPTCHA.

b. Created an "Answer Database" by having its employees and agents read tens of thousands of CAPTCHA Challenges (or listen to audio CAPTCHA Challenges) and enter the answers into a database of File IDs and corresponding answers.

12. It was further part of the conspiracy that, during the ticket-buying process, instead of "reading" a CAPTCHA Challenge, the CAPTCHA Bots identified the CAPTCHA Challenge's File ID. The CAPTCHA Bots then instantly compared the CAPTCHA Challenge's File ID against the Answer Database, looking for a matching File ID. If the CAPTCHA Bots found a matching File ID, it immediately and automatically transmitted the pre-typed answer to that CAPTCHA Challenge to the Online Ticket Vendors' website. This process took place in a fraction of a second, much faster than a human user could respond to a typical CAPTCHA Challenge.

13. It was further part of the conspiracy that the CAPTCHA Bots would impersonate visually impaired customers attempting to buy tickets by matching audio CAPTCHA Challenges from the Online Ticket Vendors against the Answer Database.

Deceptive Techniques

14. It was further part of the conspiracy that, to disguise Wiseguys' operations from the Online Ticket Vendors, defendants LOWSON and KIRSCH directed that the CAPTCHA Bots be programmed to

buy tickets in a "Human Realistic" fashion, that is, by mimicking steps that a human would use to purchase a ticket. "Human Realistic" pulling, for example, included programming the CAPTCHA Bots to make mistakes – a trick that would make an automated transaction appear to be human.

15. It was further part of the conspiracy that Wiseguys purchased tickets using thousands of different IP Addresses to create the illusion that different individual customers or households were using different computers throughout the United States to buy Event tickets online. To this end, defendants LOWSON, KIRSCH, and STEVENSON sought to register 100,000 IP addresses throughout the United States to buy Event tickets online (the "IP Bank").

16. It was further part of the conspiracy that defendants LOWSON, KIRSCH, and STEVENSON would create the illusion that the IP Bank was not leased to one company (i.e., Wiseguys) by leasing IP addresses for the IP Bank that were non-consecutive. (Companies typically lease consecutive IP addresses for ease of administration.)

17. It was further part of the conspiracy that defendants LOWSON and KIRSCH developed the IP Bank to have extra IP addresses available in case Online Ticket Vendors blocked particular IP addresses as being linked to automated purchases.

18. It was further part of the conspiracy that Wiseguys would hide the Watchers (described above in paragraph 10(a)) to prevent their detection by the Online Ticket Vendors. To this end, Wiseguys leased servers anonymously on an hourly basis from Amazon.com. Wiseguys terminated the Watchers' leases with Amazon.com as soon as the Watchers detected that tickets were available, effectively erasing the Watchers and concealing any link between the Watchers and Wiseguys' ticket purchases that followed.

19. It was further part of the conspiracy that when the Online Ticket Vendors permitted "pre-sales" to particular fan clubs or other groups (e.g., Apple iTunes users), Wiseguys employees would register for the fan clubs using fake names and fake e-mail accounts in an attempt to mask the fact that it was Wiseguys, and not regular consumers, attempting to purchase tickets.

Using Credit Cards to Impersonate Buyers

20. It was further part of the conspiracy that Wiseguys would require brokers to provide as many as 150 credit card numbers and corresponding account holder names and addresses across the United States, including those of New Jersey account holders, for use by the CAPTCHA Bots in purchasing Event tickets. The account holders were rarely, if ever, the individuals for whom the CAPTCHA Bots purchased Event tickets. By requiring

brokers to provide numerous credit card numbers and related account information, Wiseguys sought to further the false appearance that the ticket purchasers were human beings in the Primary Market.

21. It was further part of the conspiracy that defendants LOWSON and KIRSCH directed Wiseguys employees to obtain credit cards in their own names so that the CAPTCHA Bots could use those credit cards to purchase tickets, even though nearly all of the ticket purchases were intended for resale to ticket brokers.

Preparing to Purchase Tickets

22. It was further part of the conspiracy that, prior to Event sales on Online Ticket Vendors' websites, Wiseguys employees would solicit orders from ticket brokers. Wiseguys did not limit its customers to any particular number of tickets and permitted its clients to specify seat and section preferences for each venue.

23. It was further part of the conspiracy that, prior to each ticket sale, Wiseguys employees would "build" each show by programming the CAPTCHA Bots to search for only the tickets that Wiseguys' broker clients requested or that Wiseguys employees believed could be sold at a mark-up to ticket brokers.

24. It was further part of the conspiracy that when Event tickets went on-sale, the CAPTCHA Bots would seize a number of prize seats, which Wiseguys' employees would then cull through to

select and purchase the best available seats. Wiseguys employees did not have to navigate to Online Ticket Vendors' webpages or complete any aspect of the ticket-purchasing process other than the selection of which seats to purchase.

Selecting and Purchasing the Tickets

25. It was further part of the conspiracy that, when the CAPTCHA Bots seized the best available seats from the Online Ticket Vendors' networks, those same tickets were unavailable for purchase or consideration by any authorized user of the Online Ticket Vendors' websites until a Wiseguys employee released those seats.

26. It was further part of the conspiracy that Wiseguys would obtain large numbers of tickets per show. Although the CAPTCHA Bots never purchased more than the permitted number of tickets allowed on an individual credit card, the CAPTCHA Bots allowed Wiseguys employees to impersonate hundreds of buyers at the same time. The CAPTCHA Bots would automatically respond to CAPTCHA Challenges on the Online Ticket Vendors' websites and click a box containing a user's acceptance of the Online Ticket Vendors' terms of service, despite the fact that Wiseguys and the CAPTCHA Bots were then violating those same terms of service.

27. It was further part of the conspiracy that the CAPTCHA Bots would cause Online Ticket Vendors to mail purchased tickets to addresses corresponding to the credit card account holders

whose cards the CAPTCHA Bots used to purchase tickets, including account holders in New Jersey and elsewhere. The account holders, by agreement with Wiseguys, would send the tickets to Wiseguys for resale to actual customers. Wiseguys then refunded the ticket prices on the credit cards it used to purchase tickets.

28. It was further part of the conspiracy that, if there were problems with tickets purchased, defendant LOWSON and others would direct Wiseguys employees to contact Online Ticket Vendors and to impersonate the credit card holders in an attempt to resolve the problems and obtain the purchased tickets.

29. It was further part of the conspiracy that Wiseguys employees did not identify themselves as Wiseguys employees, nor did they say they were calling on behalf of ticket brokers.

Negotiating Wiseguys' Profits

30. It was further part of the conspiracy that defendant LOWSON and Wiseguys employees working at his direction would negotiate charges with ticket brokers by evaluating the market price of each Event ticket purchased and agreeing upon prices above the face value of the Event ticket (hereinafter "Overs").

31. It was further part of the conspiracy that defendant LOWSON and Wiseguys established a secure broker website through which ticket brokers, including brokers in New Jersey, could

order tickets, negotiate Overs, and provide credit cards for use by the CAPTCHA Bots.

32. It was further part of the conspiracy that defendant LOWSON and Wiseguys would ultimately sell Events tickets to select ticket brokers in New Jersey and elsewhere for the face value of the event ticket plus the agreed-upon Over. The ticket brokers subsequently sold Wiseguy-purchased tickets to customers in New Jersey and elsewhere.

33. It was further part of the conspiracy that Wiseguys would charge high Overs, including Overs of approximately $1,000 per ticket, by obtaining so many of the premium tickets for an Event that Wiseguys was the leading source for the best tickets to the most popular Events.

34. It was further part of the conspiracy that in or about 2007, defendants LOWSON and KIRSCH implemented a bonus program that promised a 100-percent-of-salary bonus if Wiseguys employees met the company's goal of purchasing one million tickets in that calendar year. Only tickets with Overs greater than approximately $20 would count towards the one-million ticket goal.

Additional Acts of Concealment and Manipulation

35. It was further part of the conspiracy that defendants KIRSCH, LOWSON, and STEVENSON directed S.W. to establish a voicemail system for Wiseguys containing as many as 1000

seemingly unrelated telephone numbers that could be given out to Online Ticket Vendors to create the appearance that the telephone numbers belonged to individual ticket purchasers and not Wiseguys.

36. It was further part of the conspiracy that defendants LOWSON and KIRSCH would direct what they referred to as "stealth measures" to avoid being detected by the Online Ticket Vendors. Specifically, Wiseguys would, among other things:

a. rent real estate using the name Smaug;

b. rent IP addresses for use with the CAPTCHA Bots in false individual and false company names;

c. rent a mail drop in Las Vegas, Nevada despite having no office presence in that state;

d. instruct employees not to identify the Wiseguys' offices as being in San Francisco; and

e. limit what information employees could disclose about Wiseguys to future employers.

37. It was further part of the conspiracy that defendant KIRSCH would obtain IP addresses for use by the CAPTCHA Bots by falsely telling the companies that owned those IP addresses that his company tested internet protocols or provided hotel room brokering services.

38. It was further part of the conspiracy that when Wiseguys would receive a cease and desist letter from

Ticketmaster or another Online Ticket Vendor relating to its activities, defendants LOWSON, KIRSCH, and STEVENSON would modify the CAPTCHA Bots in an effort to remain hidden while continuing to use the CAPTCHA Bots to buy tickets.

39. It was further part of the conspiracy that defendants LOWSON and others would conceal from their employees and the Contract Hackers efforts that Ticketmaster had taken to limit Wiseguys' use of automation to purchase Event tickets, including the sending of cease and desist letters and calls Wiseguys received from Ticketmaster.

40. It was further part of the conspiracy that when employees inquired about legal actions that Ticketmaster had taken against companies using OCR and automation to purchase Event tickets, defendant LOWSON would tell them that OCR was wrong and then misrepresent that Wiseguys did not use OCR.

Renaissance Events Management

41. It was further part of the conspiracy that, in or about 2008, having damaged the Online Ticket Vendors' ability to distribute Event tickets fairly on a first-come, first-served basis, defendants LOWSON and KIRSCH would establish and operate Renaissance Events Management ("REM"), a company that proposed to sell Event tickets on behalf of artists and venues as a competitor of Online Ticket Vendors.

42. It was further part of the conspiracy that defendant LOWSON would profit by holding REM out to be a company that could keep tickets out of the hands of brokers – that is, REM could eliminate the very interference with the Primary Market that he, Wiseguys, and defendants KIRSCH, STEVENSON, and NAHDI had created. Specifically, REM's business plan stated that the company would "follow through with the intent of presales by making sure fans get the seats, increasing fan appreciation."

OVERT ACTS

In furtherance of the conspiracy and to effect its unlawful object, defendants LOWSON, KIRSCH, STEVENSON, and NAHDI; Wiseguys; and others committed and caused to be committed the following overt acts in the District of New Jersey and elsewhere:

Pursuing Automated Ticket Purchasing

43. Defendants LOWSON, KIRSCH, and STEVENSON discussed and implemented with P.S. and others means of purchasing tickets automatically without responding to CAPTCHA Challenges:

a. On or about August 8, 2003, defendant LOWSON told P.S. via Internet chat that defendants LOWSON, KIRSCH, and STEVENSON had agreed that Wiseguys should pursue further "non-human" means of purchasing tickets.

b. On or about January 9, 2009, defendant LOWSON received an e-mail from F.F. indicating that reCAPTCHA might change the audio files it used to generate audio CAPTCHA Challenges. LOWSON replied, "is there another back door at TM or maybe a review of potentials is in order."

c. On or about January 11, 2009, defendants KIRSCH and LOWSON exchanged e-mails regarding changes in reCAPTCHA. Defendant KIRSCH suggested using OCR. Defendant LOWSON replied: "first things first we need to know if a site has backdoors or not thanks." Later on or about January 11, 2009, defendant LOWSON stated in an e-mail to defendant KIRSCH "The reasons I

believe that knowing if a site has a backdoor first or not is best . . . We have only survived with one . . ."

d. On or about January 16, 2009, S.G. sent an e-mail to defendant KIRSCH outlining the "backdoors" and "tricks" that Wiseguys had used to obtain tickets from the Online Ticket Vendors Ticketmaster, LiveNation, Tickets.com and Major League Baseball.

e. On or about January 24, 2009, defendant LOWSON sent an e-mail to defendant KIRSCH and other Wiseguy employees with the subject "Importance of way not to type." In the e-mail, defendant LOWSON stated: "We must not underestimate the importance of figuring out a way to pull sites without typing."

Efforts to Defeat CAPTCHA by OCR

44. Defendants LOWSON, KIRSCH, and STEVENSON; P.S.; and others discussed and implemented strategies to defeat CAPTCHA using OCR:

a. On or about August 10, 2006, P.S. sent an e-mail to defendants LOWSON and KIRSCH under the subject line: "Regarding pulling new sites." In the e-mail, P.S. discussed OCR techniques used to pull tickets from Musictoday and Telecharge: "For Musictoday, a hack is currently available that allows one to know the letters on the image and thus bypass it. This is because they goofed in a pretty weird way, this may not hold for a long

time. At least partial OCR may also be possible for Musictoday from the guy that does the Telecharge OCR for us."

b. On or about September 30, 2006, P.S. received computer code for using OCR on Telecharge's website to obtain tickets automatically and to defeat CAPTCHA Challenges. P.S. wrote in an Internet chat to defendant LOWSON: "We have the OCR software for Telecharge, and tomorrow I will start working on the Telecharge puller for real."

c. On or about October 1, 2006, P.S. reported to defendant LOWSON that "current TM images are 100% within the reach of a capable OCR developer." Defendant LOWSON instructed P.S. to look for a programmer capable of defeating Ticketmaster's CAPTCHA through OCR.

d. On or about October 10, 2006, P.S. reported to defendant LOWSON that he had obtained and reviewed the source code for Ticketmaster's CAPTCHA image distortion process and determined that OCR was possible if Wiseguys were to hire the "right guy."

e. On or about October 10, 2006, P.S. obtained the source code for Telecharge's CAPTCHA implementation and reported to defendant LOWSON: "Through hacks we were able to obtain the source code Telecharge uses to distort its images. . . . Therefore I decided to move forward with looking for a guy and using the task as a test for his abilities. . . . At the end,

the price estimation was right and the OCR rate was as predicted because the images were indeed as easy to OCR as the initial hacks have predicted. Therefore the best option is to do hacks on a daily basis and be able to call academic OCR help in case all hacking options have been exhausted."

f. In or about 2007, defendant STEVENSON posted the Telecharge CAPTCHA source code to an internal website used by Wiseguys.

g. On or about January 25, 2009, P.S. told defendants LOWSON and KIRSCH, and others, that "[t]he images on Tickets.com can be OCR'd, much the same way I broke them many years ago when we first tried to pull that site." Defendant LOWSON replied: "Beautiful Thanks."

Building and Operating the CAPTCHA Bots

45. Defendants LOWSON, KIRSCH, STEVENSON, and NAHDI developed and operated the CAPTCHA Bots with others and updated the Answer Database when Wiseguys encountered new CAPTCHA Challenges:

a. In or about July 2007, defendant STEVENSON wrote a computer program intended to defeat Ticketmaster's Proof-of-Work security mechanism.

b. On or about May 2, 2008, defendant NAHDI instructed Wiseguys employees, at defendant LOWSON's direction, that "audio

typing is the first priority to work on unless there is assignment requires dead line [sic]."

c. On or about May 2, 2008, defendant NAHDI instructed Wiseguys employees, at defendant LOWSON's direction, that audio typing needed to be performed for a full day on Saturday, May 3, 2008 and Sunday, May 4, 2008.

d. On or about May 22, 2008, defendant NAHDI instructed Wiseguys employees that "auto pulling is off again. We have about 45K audio files to type. Please make extra efforts to use your time to focus on this."

Hiding Wiseguys' Operations and Avoiding IP Blocks

46. Defendants LOWSON, KIRSCH, STEVENSON, and NAHDI used aliases, shell companies, and false statements to conduct Wiseguys' operations:

a. On or about March 27, 2007, defendant LOWSON instructed Wiseguys employees to use the name "Smaug" (and not Wiseguys) on all correspondence: "to be safe please confirm that the physical address in SF will not receive mail under Wiseguy and that any mail received should be Smaug only thanks."

b. On and prior to September 14, 2007, defendants NAHDI and KIRSCH administered Wiseguys' registration for approximately 999 Internet domain names, such as www.barbecuebands.com and www.airportfanclub.com, that were used to generate thousands of

e-mail addresses to purchase tickets surreptitiously and to register for fan clubs.

c. On or about January 14, 2008, defendant KIRSCH, using the alias Robert Woods and representing himself to be an employee of a shell company, "Platinum Technologies," contacted several companies that offered offsite Internet connections ("Colocation Facilities"), requesting proposals for computer hosting services.

d. In or about February 2008, defendant KIRSCH, again posing as Robert Woods, falsely told a representative of a Colocation Facility that he needed a broad array of computers because his company was engaged in a content delivery system for a hotel room brokering business.

e. On or about June 3, 2008, defendants LOWSON and KIRSCH exchanged e-mails relating to a call Wiseguys received from a Ticketmaster representative. Defendant LOWSON stated: "first of all, see if this guy has some hard statistics on your pull[. I]f he does not have any, bullshit him to think that you are a smaller player than you currently are." Defendant LOWSON later suggested either impersonating an attorney in the call to Ticketmaster or having defendant NAHDI impersonate a caller from India.

f. On or about June 5, 2008, defendant NAHDI forwarded to defendant KIRSCH a cease and desist letter from an Internet Service Provider to a Mr. Chris Karl, a false name under which

Wiseguys leased IP addresses ("The June 5 Cease and Desist"). The June 5 Cease and Desist instructed Wiseguys to "immediately cease and desist any and all connections to ticketmaster.com and their associated IP range from your ... colocation account."

g. On or about June 6, 2008, defendants LOWSON, KIRSCH, and STEVENSON engaged in an e-mail discussion under the subject line "The Future of Pulling." Defendant LOWSON advised Wiseguys employees to use corporate aliases and servers in different locations to operate the CAPTCHA Bots: "Different Company/Contact Info Per Colocation - use the 1000 phone # setup for fastest knowledge of issue with collocation [sic]." Later in the same e-mail, defendant LOWSON stated that "TM will send a letter to a colocation prior to further action if they cannot locate who owns the unit or think it is a different firm - super important."

47. Defendants LOWSON, KIRSCH, and STEVENSON directed Wiseguys' operations in an effort to avoid having the CAPTCHA Bots discovered and blocked by the Online Ticket Vendors:

a. On or about July 16, 2007, P.S. sent defendant KIRSCH an e-mail indicating that Wiseguys should consider using the CAPTCHA Bots at "faster than human" speeds. To make pulling still appear human, P.S. stated that Wiseguys would "try sending TM wrong keystroke data, that is, pretend that we are typing the

image humanly slow character by character, whereas in fact we submit it faster."

b. On or about March 2, 2008, defendant STEVENSON informed defendant LOWSON, defendant KIRSCH, and others, that Ticketmaster had blocked approximately 1,200 more IP addresses and that all "pulling" should be stopped until Wiseguys could determine the reason for the blocks.

c. On or about June 14, 2008, defendants LOWSON, KIRSCH, and STEVENSON exchanged e-mails with P.S. and others regarding the setup of IP addresses. As part of the exchange, P.S. stated: "Please note that any set of IPs is worth a good price if they are totally independent from one another, that is, when looked up in various databases, they do not belong to the same person. Otherwise, TM can just block all of them in a single sweep."

d. On or about October 2, 2007, defendant LOWSON sent an e-mail to Wiseguys employees stating: "A few loose lips out there please keep below in mind. 'How we do things is none of anyone's business.' This should be your standard response when someone asks about our operation."

e. On or about September 15, 2008, F.F. sent an e-mail to defendants LOWSON, KIRSCH and STEVENSON. In it, F.F. discussed the use of the 100,000-address IP Bank to get around Ticketmaster's blocks. In particular, he stated "Regarding latest TM blocks here is the new explicit stealth protocol: 1. We

employ full stealth (even at the expense of not completing something) without debate until we get our 100k IP setup. 2. Once we have the large IP setup, stealth is full employed 100% unless agreed to a change." In response, defendant KIRSCH chastised F.F. for talking about the plan for 100,000 IP's with everyone, stating, "This gave away too much to too many people who aren't even cleared to know about our 100k IP plan."

f. On or about September 30, 2008, in response to complaints by B.C. that he had been getting blocked by Ticketmaster, defendant KIRSCH instructed B.C. to use Internet proxies - servers that act as an intermediary between two computers, and can be used to maintain anonymity on the Internet – in accessing Ticketmaster to avoid getting blocked.

Securing Premium Tickets to Popular Events

48. Defendants LOWSON, KIRSCH, STEVENSON, and NAHDI secured premium tickets to popular events:

a. On or about November 11, 2005, defendant LOWSON boasted to P.S. that when 1,000 Rose Bowl tickets were released for the BCS Football Championship Game (that would later take place between Texas and the University of Southern California), Wiseguys was able to purchase 882 tickets. Referring to Online Ticket Vendors' efforts to cancel purchases made using automation, LOWSON stated, "Biz as usual, no cancels."

b. On or about June 19, 2006, Wiseguys used the CAPTCHA Bots to purchase at least approximately 136 Barbara Streisand tour tickets.

c. On or about September 10, 2007, Wiseguys used the CAPTCHA Bots to purchase approximately 229 premium tickets for the October 9 and 10, 2007 Bruce Springsteen concerts at the Continental Arena in East Rutherford, New Jersey.

d. In or about September 2007, defendants KIRSCH and STEVENSON supervised an effort to purchase tickets for Yankees playoff games by registering for the Yankees ticket lottery, which expressly limited ticket purchases to two per person. As a result of their efforts, on or about September 26, 2007, Wiseguys obtained approximately 1,250 ticket purchase codes which were later used to purchase tickets.

e. On or about September 27 and 28, 2007, Wiseguys used the CAPTCHA Bots and the ticket purchase codes described above to purchase approximately 1,924 Yankees tickets for anticipated playoff games with a total face value of approximately $159,000.

49. Defendant KIRSCH and others acting at his direction registered false names and e-mail addresses to obtain pre-sale passwords that could be used to purchase tickets for various Hanna Montana/Miley Cyrus concerts, and later purchased those tickets:

a. On or about August 6, 2007, in advance of ticket sales for a Miley Cyrus concert, defendant KIRSCH directed defendant STEVENSON, O.M., and F.F. to register 200 users to the Miley Cyrus website www.mileyworld.com using credit cards under Wiseguys' control.

b. On or about August 7 and 8, 2007, defendant KIRSCH directed O.M. to register an additional 600 users to www.mileyworld.com using the same credit card numbers.

c. Between on or about August 18, 2007 and on or about December 1, 2007, Wiseguys used the CAPTCHA Bots to purchase at least approximately 11,984 tickets for various Hannah Montana tour shows in the United States, with a total face value of approximately $916,000.

d. Between in or about September 2007 and December 2007, Wiseguys used the CAPTCHA Bots to purchase approximately 300 premium tickets for the December 29 and 30, 2007 Hannah Montana concerts at the Prudential Center in Newark, New Jersey, with a total face value of approximately $24,000.

The 2008 Bruce Springsteen Tour

50. Between on or about September 8, 2007 and December 15, 2007, Wiseguys used the CAPTCHA Bots to purchase at least approximately 11,728 tickets for various Bruce Springsteen tour shows in the United States, with a total face value of approximately $1,284,000. Of these tickets, approximately 1,497

(with a total face value of approximately $168,000) were for the Bruce Springsteen concerts on July 27, 28, and 31, 2008 at Giants Stadium in East Rutherford, New Jersey.

a. As set forth in the table below, the CAPTCHA Bots purchased consecutively numbered seats in the most desirable sections of Giants Stadium for the July 28 concert. For example, in seven separate transactions purporting to have been conducted by seven different individuals, the CAPTCHA Bots purchased all of the seats between Seats 13 and 34 in General Admission ("GA") Section 1 – one of the areas closest to the stage – and permitted no other customers to buy tickets in that seat range.

b. For the July 28 concert, Wiseguys used the CAPTCHA Bots to purchase approximately 635 premium tickets in the GA area and in other premium seating areas by directing the CAPTCHA Bots to impersonate individual human ticket purchasers and by providing Ticketmaster with false, Wiseguy-controlled e-mail addresses and credit cards, including, among others, the purchasers and e-mail addresses listed below:

[illegible]	Row	[illegible]	[illegible]	[illegible]
GA PIT	GA1	13-16	[R.B.]	PQFG1@anetnet.com
GA PIT	GA1	17-20	[B.G.]	[B.G.]@letsjamsportswithoutspam.com
GA PIT	GA1	21-22	[M.J.]	[J.M]@myveryownsiteandpersonalemail.com
GA PIT	GA1	23-26	[C.B.]	[C.B.]@maildirectoryathletics.com
GA PIT	GA1	27-30	[D.M.]	[D.M.]@simplepeoplesitesforfree.com

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
GA PIT	GA1	31-32	[D.B.]	[B.J.]@latinowebemailamundo.com
GA PIT	GA1	33-34	[P.A.]	[P.A.]@freemailsitebaseball.com
GA PIT	GA1	39-42	[M.G.]	[M.G.]@myfantasyteamrulez.com
GA PIT	GA1	43-46	[P.B.]	[P.B.]@stupidcellphone.com
GA PIT	GA1	47-50	[J.D.]	[J.D.]@asiansinglesonlineusa.com
GA PIT	GA2	1-4	[K.P.]	[P.K.]@phoenixshufflenet.com
GA PIT	GA2	5-8	[D.W.]	[W.D.]@bushloversvotedicknext.com
GA PIT	GA2	9-10	[T.P.]	[P.T.]@simpleinternetlistings.com
GA PIT	GA2	18-21	[W.G.]	[W.G.]@freemailfreesitefreedom.com
GA PIT	GA2	26-29	[M.R.]	[M.R.]@allowmailnetservices.com
GA PIT	GA2	30-33	[E.P.]	[P.E.]@bushloversvotedicknext.com
GA PIT	GA2	34-37	[B.W.]	[D.W.]@scifiandthesportsguy.com
GA PIT	GA2	38-41	[C.J.]	[C.J.]@bushloversvotedicknext.com
GA PIT	GA2	42-43	[F.W.]	[F.W.]@blasterpackemail.com
GA PIT	GA2	44-47	[D.O.]	[O.D.]@imagine-freedominmail.com
1	2	3-4	[A.N.]	[A.N.]@simpleinternetlistings.com
1	5	1-2	[S.J.]	[S.J.]@bushloversvotedicknext.com
1	5	17-20	[E.R.]	speedy7@piration.org
1	5	25-26	[T.P.]	[P.T.]36@thebosslinxandblogz.com
1	6	5-8	[A.M.]	[M.A.]@myfantasyteamrulez.com
2	2	15-16	[B.E.]	[B.E.]@freemailfreesitefreedom.com
2	4	7-10	[J.E.]	[C.B.]@netslatepopmail.com
2	11	10-13	[A.C.]	[C.A.]@simpleinternetlistings.com
2	21	1-4	[S.S.]	Boroughsshani60@ffmroommaterentalservicesusa.com
3	19	4-7	[J.E.]	mnr@anetnet.com
4	4	21-24	[J.N.]	[J.N.]@ireview-liveevents.com

c. Of the approximately 440 GA tickets, which were the closest available to the stage for the above concert (and therefore among the most desirable tickets), Wiseguys used the CAPTCHA Bots to purchase approximately 220 – or 50 percent – of them.

51. Wiseguys also used the CAPTCHA Bots to purchase tickets to thousands of other Events nationwide, including, but not limited to:

Event / Artist	Venue / Location	Approximate Event Dates
Detroit Tigers, American League Championship Series	Comerica Park Detroit, Michigan	10/13/2006
The Producers	Merriam Theatre Philadelphia, Pennsylvania	11/2006
Wicked	Gerswhin Theatre New York, New York	2007-2009
Wicked	Pantages Theatre Los Angeles, California	2007
Chicago White Sox	U.S. Cellular Field Chicago, Illinois	06/2007
Kenny Chesney	Heinz Field Pittsburgh, Pennsylvania	06/9/2007
The Police	Dodger Stadium Los Angeles, California	06/23/2007
Joel Osteen	Verizon Wireless Washington, D.C.	07/20/2007
Kelly Clarkson	Izod Center E. Rutherford, New Jersey	08/22/2007
Bon Jovi	Prudential Center Newark, New Jersey	10/25/2007

Event / Artist	Venue / Location	Approximate Event Dates
Tim McGraw	Cruzan Amphiteatre West Palm Beach, Florida	05/2008
U.S. Open Tennis	Arthur Ashe Stadium New York, New York	08/2008 - 09/2008
Philadelphia Eagles v. Washington Redskins	Lincoln Financial Field Philadelphia, Pennsylvania	10/05/2008
Cleveland Browns v. New York Giants	Cleveland Browns Stadium Cleveland, Ohio	10/13/2008
Sugar Bowl	Louisiana Superdome New Orleans, Louisiana	01/01/2009

52. Overall, in or about 2005, Wiseguys used the CAPTCHA Bots to purchase approximately 239,000 tickets from Online Ticket Vendors and made approximately $5.9 million in profits on gross revenues of approximately $24 million.

53. In or about 2006, Wiseguys used the CAPTCHA Bots to purchase approximately 411,000 tickets from Online Ticket Vendors and made approximately $8.4 million in profits on gross revenues of approximately $41.5 million.

54. In or about 2007, Wiseguys used the CAPTCHA Bots to purchase approximately 700,000 tickets from Online Ticket Vendors and made approximately $9.2 million in profits on gross revenues of approximately $50 million.

55. Through November 2008, Wiseguys used the CAPTCHA Bots to purchase at least approximately 166,000 tickets from Online Ticket

Vendors that generated at least approximately $5.4 million in profits for the calendar year 2008.

"Dominating" the Market

56. At defendant LOWSON and defendant KIRSCH's direction, Wiseguys employees used the CAPTCHA Bots to impersonate as many as 1,400 individual ticket buyers interested in purchasing tickets for popular Events and thereby made unavailable to the rest of the ticket-buying public many of the best seats to these Events as Wiseguys employees decided which of the best Event tickets to purchase:

a. In a February 25, 2007 e-mail, P.S. advised defendant LOWSON how to use pricing strategy to maintain Wiseguys' market position:

> It may also be a good idea to ask your trusted brokers if the situation has changed for the buying public once you monopolized the market. In other words, I suspect that in the past there were [sic] some opportunity for normal people with a macro and an internet exporer [sic] to score a few quite good tickets for themselves and event flip them on ebay. This is probably no longer the case, therefore such people are either forced to buy worse seats from TM once you have got all the best, or must now use brokers to get the good seats. Such a situation would increase the sense of unfairness normal people already have and if you raise your overs and the brokers raise prices in return, this will result in more newspaper articles, more fan-club-only presale schemes and more TM action that [sic] you can possibly handle. So, whenever you think about pricing, please also think that you are a monopoly not just for your brokers, but for their clients as well - those small clients no longer have the opportunity to score on their own on the web and feel vindicated. If you do 1 million in tickets in 2007, this means that 1 million people will be displaced from the seats they deserved and further 1

> million will pay far more for the seat they are in than they are supposed to. Both groups may have some overlap in people that are both displaced and then bought a seat from a broker, however nevertheless this is a huge number so any dollar in price increase on your part that is not entirely absorbed by the brokers and passed on to the end customer will sort of multiply the animosity towards all parties involved. I would suggest that you try to contain your price haggling between you and the brokers, because if you overstep a certain phycological [sic] threshold (where it is exactly is not known), TM and the general public may snap and kill your business overnight. Maybe you should team up with your brokers and order a marketing research and polls on end customers and how much more they can handle.

b. On or about October 4, 2008, Wiseguys used the CAPTCHA Bots to impersonate 680 individual ticket buyers for the AC/DC concert at the St. Pete Times Forum in Tampa, Florida on or about December 21, 2008, and thereby held as many as 680 separate sets of tickets for that show while Wiseguys employees considered which of the most desirable tickets to purchase. Ultimately, Wiseguys used the CAPTCHA Bots to purchase 245 tickets to this event.

c. On or about October 10, 2008, Wiseguys used the CAPTCHA Bots to impersonate approximately 450 individual ticket buyers for the Coldplay concert at the Honda Center in Anaheim, California on or about November 25, 2008, and thereby held as many as 450 separate sets of tickets for that show while Wiseguys employees considered which of the most desirable tickets to purchase. Ultimately, Wiseguys used the CAPTCHA Bots to purchase approximately 122 tickets to this event. In an internal Wiseguys report regarding this Event, B.C. stated that Wiseguys got the

best available tickets for the event, stating that there was "[n]othing better listed."

d. On or about October 25, 2008, Wiseguys used the CAPTCHA Bots to impersonate approximately 800 individual ticket buyers for the AC/DC Concert at the Qwest Center in Omaha, Nebraska on or about January 15, 2009, and thereby held as many as 800 sets of tickets while Wiseguys employees considered which of the most desirable tickets to purchase. Ultimately, Wiseguys used the CAPTCHA Bots to purchase approximately 331 tickets to this show. In an internal Wiseguys report regarding this Event, B.C. stated that all the tickets were "lowers" (i.e., nearer to the stage), and described Wiseguys' ticket purchase as "Straight Domination."

e. On or about October 18, 2008, Wiseguys used the CAPTCHA Bots to impersonate approximately 1,400 individual ticket buyers (per show) for the Phish 3-Day Event Package at the Hampton Coliseum in Hampton, Virginia on or about March 6 and 7, 2009, and thereby held as many as 1,400 sets of tickets while Wiseguys employees considered which of the most desirable tickets to purchase. Ultimately, Wiseguys used the CAPTCHA Bots to purchase approximately 2,500 tickets to these Events. In an internal Wiseguys report regarding this purchase, B.C. stated: "From what I heard and talked to other guys about was that everyone had a hard time pulling it and it sold out instantly."

f. On or about November 8, 2008, Wiseguys used the CAPTCHA Bots to impersonate approximately 800 individual ticket buyers for a Wrestlemania event at Reliant Stadium in Houston, Texas on or about April 5, 2009, and thereby held as many 800 sets of tickets while Wiseguys employees decided which of the most desirable tickets to purchase. Ultimately, Wiseguys used the CAPTCHA Bots to purchase approximately 134 tickets to this event. In an internal Wiseguys report regarding this purchase, B.C. stated that Wiseguys obtained "the Best ringsides by far. We filled the lower level order and bought like 50 in the first 10 of the floor."

g. On or about November 8, 2008, Wiseguys used the CAPTCHA Bots to impersonate approximately 500 individual ticket buyers for the Billy Joel concert at the Hard Rock Live in Hollywood, California on or about January 2, 2009, and thereby held as many as 500 sets of tickets while Wiseguys employees decided which of the most desirable tickets to purchase. Ultimately, Wiseguys used the CAPTCHA Bots to purchase 68 tickets for this Event. In an internal Wiseguys report regarding this Event, B.C. described the ticket purchases by stating "Nothing better than ours."

h. On or about November 10, 2008, Wiseguys used the CAPTCHA Bots to impersonate approximately 630 individual ticket buyers for the Samsung Eternity Presents Dancing with the Stars at the Staples Center in Los Angeles, California on or about December 27, 2008, and thereby held as many as 630 sets of tickets while

Wiseguys employees decided which of the most desirable tickets to purchase. Ultimately, Wiseguys used the CAPTCHA Bots to purchase 43 tickets to this Event. In an internal Wiseguys report regarding this Event, B.C. stated that Wiseguys "[d]ominated" the ticket purchase and bought the "[b]est seats by far[:] tables and lowers."

i. On or about January 13, 2009, Wiseguys used the CAPTCHA Bots to impersonate approximately 600 individual ticket buyers for the Dave Matthews Band concert at the Izod Center in East Rutherford, New Jersey on or about April 15, 2009, and thereby held as many as 600 sets of tickets while Wiseguys employees decided which of the most desirable tickets to purchase. Ultimately, Wiseguys used the CAPTCHA Bots to purchase 216 seats for this Event.

j. In or about January 2009, Wiseguys used the CAPTCHA Bots to impersonate 1,000 individual ticket buyers for the New York Giants-Philadelphia Eagles NFL playoff game at Giants Stadium in East Rutherford, New Jersey on or about January 11, 2009, and thereby held as many as 1,000 sets of tickets while Wiseguys employees decided which of the most desirable tickets to purchase. In an internal Wiseguys report regarding this Event, B.C. stated that Wiseguys "pigged out, there were tons of seats listed."

In violation of Title 18, United States Code, Section 371.

COUNTS 2 through 10
18 U.S.C. §§ 1030(a)(2)(C) & (c)(2)(B)(i)
18 U.S.C. § 2
Obtaining Information from a Protected Computer

1. The allegations set forth in paragraphs 1 and 2 and paragraphs 5 through 56 of Count One of this Indictment are realleged and incorporated as if set forth herein.

2. On or about the dates listed below, in California, in the District of New Jersey, and elsewhere, defendants

KENNETH LOWSON,
a/k/a "Money,"
KRISTOFER KIRSCH,
a/k/a "Robert Woods," and
JOEL STEVENSON

did knowingly and intentionally access computers without authorization and exceed authorized access, and using an interstate or foreign communication, obtained information from protected computers, namely the network owned by Ticketmaster used in and affecting interstate and foreign commerce and communication, for purposes of commercial advantage and private financial gain, namely the purchase for resale of tickets to the Events listed below.

Count	Approximate Date	Event	Approximate Number of Tickets
2	6/29/2006	Barbara Streisand United Center (Chicago) 11/7/2006	50

Count	Approximate Date	Event	Approximate Number of Tickets
3	9/27/2007	2007 Yankees A.L. Division Series (New York) Game 3	368
4	9/28/2007	2007 Yankees A.L. Championship Series (New York) Game 2	290
5	9/29/2007	Hannah Montana Prudential Center (New Jersey) 12/29/07	124
6	9/29/2007	Hannah Montana Prudential Center (New Jersey) 12/30/07	136
7	12/4/2007	Rose Bowl Pasadena, California 01/01/2008	100
8	12/15/2007	Bruce Springsteen Giants Stadium (New Jersey) 7/27/2008	382
9	12/15/2007	Bruce Springsteen Giants Stadium (New Jersey) 7/28/2008	635
10	12/15/2007	Bruce Springsteen Giants Stadium (New Jersey) 7/31/2008	480

In violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(i) (West 2008 ed.), and Section 2.

COUNTS 11 through 20
18 U.S.C. §§ 1030(a)(4) & (c)(3)(A)
18 U.S.C. § 2
Accessing a Protected Computer with Intent to Defraud

1. The allegations set forth in paragraphs 1 and 2 and paragraphs 5 through 56 of Count One of this Indictment are realleged and incorporated as if set forth herein.

2. On or about December 15, 2007, in California, in the District of New Jersey, and elsewhere, defendants

KENNETH LOWSON,
a/k/a "Money,"
KRISTOFER KIRSCH,
a/k/a "Robert Woods," and
JOEL STEVENSON

did knowingly and with intent to defraud, access protected computers, namely the network owned by Ticketmaster used in and affecting interstate and foreign commerce and communication, without authorization, and exceeded authorized access, and by means of such conduct furthered the intended fraud and obtained things of value, namely the tickets described below to the July 28, 2008 Bruce Springsteen concert at Giants Stadium in New Jersey.

Count	Section	Row	Seats	Ticketmaster Account Holder Email Address
11	GA PIT	GA1	39-42	[M.G.]@myfantasyteamrulez.com
12	GA PIT	GA1	47-50	[J.D.]@asiansinglesonlineusa.com
13	GA PIT	GA2	5-8	[W.D.]@bushloversvotedicknext.com
14	GA PIT	GA2	9-10	[P.T.]@simpleinternetlistings.com
15	GA PIT	GA2	30-33	[P.E.]@bushloversvotedicknext.com
16	GA PIT	GA2	38-41	[C.J.]@bushloversvotedicknext.com

Count	Section	Box	[illegible]	[illegible]
17	1	2	3-4	[A.N.]@simpleinternetlistings.com
18	1	5	1-2	[S.J.]@bushloversvotedicknext.com
19	1	6	5-8	[M.A.]@myfantasyteamrulez.com
20	2	11	10-13	[C.A.]@simpleinternetlistings.com

In violation of Title 18, United States Code, Sections 1030(a)(4) and 1030(c)(3)(A) (West 2008 ed.), and Section 2.

COUNTS 21 through 26
18 U.S.C. § 1030(a)(5)(A)
Transmitting a Program That Causes Unauthorized Damage

1. The allegations set forth in paragraphs 1 and 2 and paragraphs 5 through 56 of Count One of this Indictment are realleged and incorporated herein.

2. On or about the dates listed below, in California, in the District of New Jersey, and elsewhere, defendants

KENNETH LOWSON,
a/k/a "Money,"
KRISTOFER KIRSCH,
a/k/a "Robert Woods," and
JOEL STEVENSON

did knowingly cause the transmission of programs, information, code, and commands, namely responses to CAPTCHA Challenges and automated ticket purchase requests, and as a result of such conduct, intentionally caused damage without authorization to protected computers, namely the network owned by Ticketmaster in and affecting interstate and foreign commerce and communication, and as a result of such conduct caused loss to one or more persons during a 1-year period aggregating at least $5,000 in value.

Count	Approximate Date	Event	Approximate Number of Users Impersonated
21	10/10/08	Coldplay Honda Center, Anaheim, California 11/25/08	450

22	10/11/08	AC/DC Qwest Center Omaha, Nebraska 1/15/09	800
23	11/8/08	Wrestlemania Reliant Stadium Houston, Texas 04/05/09	800
24	11/10/08	Dancing with the Stars Staples Center Los Angeles, California 12/27/08	630
25	01/01/2009	N.Y. Giants v. Phila. Eagles Giants Stadium East Rutherford, New Jersey 01/11/09	1,000
26	01/13/2009	Dave Matthews Band IZOD Center East Rutherford, New Jersey 04/15/09	600

In violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i), and Section 2.

COUNTS 27 through 36
18 U.S.C. § 1343
18 U.S.C. § 2
Wire Fraud

1. The allegations set forth in paragraphs 1 and 2 and paragraphs 5 through 56 of Count One are realleged and incorporated herein.

2. On or about December 15, 2007, in California, in the District of New Jersey, and elsewhere, defendants

KENNETH LOWSON,
a/k/a "Money,"
KRISTOFER KIRSCH,
a/k/a "Robert Woods,"
JOEL STEVENSON, and
FAISAL NAHDI

did knowingly and intentionally devise and intend to devise a scheme and artifice to defraud Online Ticket Vendors and others, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing such scheme and artifice to defraud, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain signs, signals, and sounds, namely responses to CAPTCHA Challenges and automated ticket purchase orders generated by the CAPTCHA Bots for the purchase of tickets described below to the July 28, 2008 Bruce Springsteen concert at Giants Stadium in East Rutherford, New Jersey.

Count	Section	Row	Seats	Alleged Email Address Used
27	GA PIT	GA1	39-42	[M.G.]@myfantasyteamrulez.com
28	GA PIT	GA1	47-50	[J.D.]@asiansinglesonlineusa.com
29	GA PIT	GA2	5-8	[W.D.]@bushloversvotedicknext.com
30	GA PIT	GA2	9-10	[P.T.]@simpleinternetlistings.com
31	GA PIT	GA2	30-33	[P.E.]@bushloversvotedicknext.com
32	GA PIT	GA2	38-41	[C.J.]@bushloversvotedicknext.com
33	1	2	3-4	[A.N.]@simpleinternetlistings.com
34	1	5	1-2	[S.J.]@bushloversvotedicknext.com
35	1	6	5-8	[M.A.]@myfantasyteamrulez.com
36	2	11	10-13	[C.A.]@simpleinternetlistings.com

In violation of Title 18, United States Code, Section 1343 and Section 2.

COUNT 37 through 43
18 U.S.C. § 1343
18 U.S.C. § 2
Wire Fraud

1. The allegations set forth in paragraphs 1 and 2 and paragraphs 5 through 56 of Count One are realleged and incorporated herein.

2. On or about the dates listed below, in California, in the District of New Jersey, and elsewhere, defendants

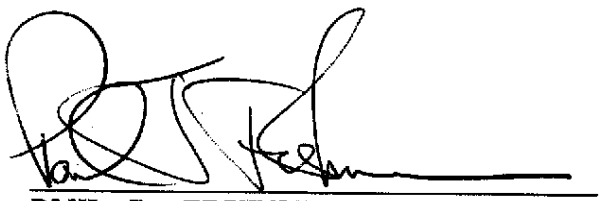
KENNETH LOWSON,
a/k/a "Money,"
KRISTOFER KIRSCH,
a/k/a "Robert Woods,"
JOEL STEVENSON, and
FAISAL NAHDI

did knowingly and intentionally devise and intend to devise a scheme and artifice to defraud Online Ticket Vendors and others, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing such scheme and artifice to defraud, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain signs, signals, and sounds, namely electronic mail messages between the defendant listed below and the individual in New Jersey listed below.

Count	Defendant	Recipient /Sender	Date	Subject
37	KENNETH LOWSON	[L.P.]	03/30/06	E-mail directing Wiseguys to seek to purchase "visually impaired seats, they are second row dead center
38	KENNETH LOWSON	[L.P.]	06/19/06	E-mail setting forth agreement between Wiseguys and L.P., including Wiseguys' use of credit cards controlled by L.P.
39	KENNETH LOWSON	[L.P.]	08/25/06	E-mail from defendant Lowson stating "Just Lost 30 Seats Because of Your Shitty Cards Thanks Fucker."
40	FAISAL NAHDI	[L.P.]	05/22/07	E-mail regarding Wiseguys reimbursing L.P. for the cost of fan club memberships
41	FAISAL NAHDI	[L.P.]	07/09/07	E-mail regarding Wiseguys reimbursing L.P. $16,224.85 for the cost of fan club memberships
42	KRISTOFER KIRSCH	[D.E.] [A.R]	03/20/08	E-mail falsely portraying Wiseguys as "content distribution" company
43	KRISTOFER KIRSCH	[D.E.]	05/24/08	E-mail requesting "500,000 IPs, or dynamic proxy IP access to more than 500,000 IPs"

In violation of Title 18, United States Code, Section 1343 and Section 2.

A TRUE BILL



PAUL J. FISHMAN
UNITED STATES ATTORNEY

CASE NUMBER: 10-114(KSH)

United States District Court
District of New Jersey

UNITED STATES OF AMERICA

v.

KENNETH LOWSON,
a/k/a "Money,"
KRISTOFER KIRSCH,
a/k/a "Robert Woods,"
JOEL STEVENSON, and
FAISAL NAHDI

INDICTMENT FOR

18 U.S.C. §§ 371, 1030, 1343, and 2

PAUL J. FISHMAN
U.S. ATTORNEY NEWARK, NEW JERSEY

EREZ LIEBERMANN
SETH KOSTO
ASSISTANT U.S. ATTORNEYS
(973) 645-2874/2737

USAO#2007R001178